

# EXHIBIT J

Michelle Chua (DC Bar 441990)  
Bikram Bandy (DC Bar 480967)  
Karen S. Hobbs (DC Bar 469817)  
600 Pennsylvania Avenue, NW, CC-8528  
Washington, DC 20580  
202-326-3248 (Chua)  
202-326-2978 (Bandy)  
202-326-3587 (Hobbs)  
[mchua@ftc.gov](mailto:mchua@ftc.gov); [bbandy@ftc.gov](mailto:bbandy@ftc.gov)  
[khobbs@ftc.gov](mailto:khobbs@ftc.gov)  
Attorneys for Plaintiff  
Federal Trade Commission

**UNITED STATES DISTRICT COURT**  
**DISTRICT OF ARIZONA**

Federal Trade Commission,  
Plaintiff,

v.

Electronic Payment Solutions of America, Inc.,  
an Arizona corporation;  
Electronic Payment Services, Inc., an Arizona  
corporation;  
KMA Merchant Services, LLC, a New Jersey  
limited liability company;  
Dynasty Merchants, LLC, an Arizona limited  
liability company;  
Jay Wigdore, individually and as an officer of  
Electronic Payment Services, Inc. and  
Electronic Payment Solutions of America, Inc.;  
Michael Abdelmesseheh a/k/a Michael Stewart,  
individually and as an officer of Electronic  
Payment Solutions of America, Inc., and KMA  
Merchant Services, LLC;  
Nikolas Mihilli, individually and as an officer  
of Dynasty Merchants, LLC;  
Electronic Payment Systems, LLC, a Colorado

Case No. CV-17-02535-PHX-DJH

**FIRST AMENDED COMPLAINT  
FOR PERMANENT  
INJUNCTION AND OTHER  
EQUITABLE RELIEF**

limited liability company;  
Electronic Payment Transfer, LLC, a Colorado  
limited liability company;  
John Dorsey, individually and as an officer of  
Electronic Payment Systems, LLC and  
Electronic Payment Transfer, LLC;  
Thomas McCann, individually and as an officer  
of Electronic Payment Systems, LLC and  
Electronic Payment Transfer, LLC; and  
Michael Peterson, individually and as Risk  
Manager of Electronic Payment Systems, LLC,  
Defendants.

1 Plaintiff, the Federal Trade Commission (“FTC”), for its First Amended  
2 Complaint (“Complaint”) alleges:

3  
4 1. The FTC brings this action under Section 13(b) of the Federal Trade  
5 Commission Act (“FTC Act”), 15 U.S.C. § 53(b), and the Telemarketing and Consumer  
6 Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. §§ 6101-6108, to  
7 obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the  
8 refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for  
9 Defendants’ acts or practices in violation of Section 5(a) of the FTC Act, 15  
10 U.S.C. § 45(a), and in violation of the FTC’s Trade Regulation Rule entitled  
11 Telemarketing Sales Rule (“TSR”), 16 C.F.R. Part 310.  
12

### 13 **JURISDICTION AND VENUE**

14  
15 2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331,  
16 1337(a), and 1345, and 15 U.S.C. §§ 45(a), 53(b), 6102(c), and 6105(b).  
17

18 3. Venue is proper in this district under 28 U.S.C. § 1391(b)(2) and (c), and 15  
19 U.S.C. § 53(b).  
20

### 21 **SUMMARY OF CASE**

22 4. This is an action by the FTC for injunctive and equitable monetary relief on  
23 behalf of consumers against Defendants for their actions in laundering credit card  
24 transactions on behalf of a deceptive telemarketing scam called Money Now Funding  
25 (“MNF” or “MNF scam”). In 2013, the FTC sued MNF for telemarketing worthless  
26 business opportunities to consumers and falsely promising that consumers would earn  
27  
28

1 thousands of dollars in income. In 2015, the court entered summary judgment and default  
2 judgments against certain MNF defendants, finding the business opportunities were a  
3 complete fraud, as alleged in the complaint, and that consumers who purchased these  
4 opportunities lost thousands of dollars each, resulting in \$7,375,258.84 in total consumer  
5 injury. Each of the remaining MNF defendants settled in 2015.  
6

7         5. The principals of the MNF scam went to great lengths to hide their  
8 identities behind a large number of phony “businesses.” In order to charge consumers’  
9 credit cards but make it difficult to trace the money back to MNF, MNF engaged in a  
10 credit card laundering scheme whereby its principals and employees created numerous  
11 fictitious companies, and then Defendants processed victim credit card charges through  
12 merchant accounts established in the names of these fictitious companies, rather than  
13 through a single merchant account in the name of MNF. MNF transactions were also  
14 laundered through at least two merchant accounts set up in the name of companies  
15 created by Defendant Abdelmessehe, and one merchant account set up in the name of a  
16 business created by Defendant Mihilli.  
17

18         6. The practice of processing credit card transactions through another  
19 company’s merchant accounts is called “credit card laundering” or “factoring” in the  
20 credit card industry. It is strictly forbidden by the credit card companies and is illegal  
21 under the TSR.  
22

23         7. The banking system behind credit card processing involves a complex  
24 series of exchanges involving numerous entities. These entities include, on one side, the  
25 consumer and the consumer’s bank and, on the other, the merchant and the merchant’s  
26  
27  
28

1 bank; between them are the credit card networks (*e.g.*, VISA) and other third parties such  
2 as “independent sales organizations” involved in processing a transaction.

3 8. An independent sales organization (“ISO”) solicits merchants seeking to  
4 open credit card merchant accounts and refers them to the ISO’s acquiring bank  
5 (“acquirer”), which is the bank that has access to the credit card networks. In some cases,  
6 ISOs perform the underwriting of merchants for their acquirer and/or process consumer  
7 credit card payments on behalf of their acquirer, either directly or through the services of  
8 payment processors.  
9

10 9. Through the ISO’s relationship with acquirers, ISOs function as important  
11 gatekeepers, screening out and preventing fraudulent merchants from gaining access to  
12 the credit card networks, or identifying such merchants once they have gained access.  
13 Conversely, an ISO that is complicit with a fraudulent merchant can provide such a  
14 merchant access to the credit card networks that the merchant would not otherwise be  
15 able to obtain or maintain.  
16

17 10. Defendant Electronic Payment Systems, LLC (“EPS”) is an ISO that  
18 markets ISO and payment processing services to prospective merchants. In 2012 and  
19 2013, EPS served as the ISO for the entities involved in the MNF scam.  
20

21 11. EPS engaged in the underwriting and approval of MNF’s fictitious  
22 companies, and helped set up merchant accounts with its acquirer for these fictitious  
23 companies. Using the services of two payment processors, EPS processed more than  
24 \$5,895,035 in MNF transactions through these and other fraudulent merchant accounts.  
25  
26  
27  
28

13. Defendant Wigdore submitted the merchant applications for the MNF fictitious companies to EPS. Once EPS processed MNF's transactions through the fictitious company accounts, the MNF sales revenues were transferred to companies controlled by Defendants Wigdore, Abdelmesseih, and Mihilli, as well as participants in the MNF laundering scheme.

14. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101–6108. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

15. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 56(a)(2)(A), 6102(c) and 6105(b).

## DEFENDANTS

16. As explained below, this case involves two sets of defendants: the “KMA-Wigdore Defendants” and the “EPS Defendants” (collectively, “the Defendants”). The KMA-Wigdore Defendants are three individuals who acted as EPS’s ISO sales agents, and four entities associated with these individuals. The EPS Defendants are the ISO—which uses the names Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC—and their two principals and risk manager.

### The KMA-Wigdore Defendants

17. The KMA-Wigdore Defendants are three individuals who acted as EPS’s ISO sales agents and who directly participated in the MNF credit card laundering scheme, and four corporate entities associated with these individuals. Two of these individuals, Defendants Jay Wigdore (“Wigdore”) and Michael Abdelmesseh (“Abdelmesseh”), acted directly as EPS’s ISO sales agents. The third individual, Defendant Nikolas Mihilli (“Mihilli”), acted as a sub-agent working under Wigdore and Abdelmesseh.

18. Defendant Electronic Payment Services, Inc. (“EP Services”) is an Arizona corporation with its principal place of business at 1640 W. Prescott Dr., Chandler, Arizona 85248. At all times material to this Complaint, EP Services acted as an ISO sales agent for Defendant EPS, and referred merchants to EPS for underwriting approval and payment processing services. EP Services used various dba names, including “EPS-America.” EP Services transacts or has transacted business in this district and throughout the United States.



1           19. Defendant Electronic Payment Solutions of America, Inc. (“EPSA”) is an  
2 Arizona corporation with its principal place of business at 1048 N. 44<sup>th</sup> Street #100,  
3 Phoenix, Arizona 85008. At all times material to this Complaint, EPSA acted as an ISO  
4 sales agent for EPS, and referred merchants to EPS for underwriting approval and  
5 payment processing services. EPSA transacts or has transacted business in this district  
6 and throughout the United States.  
7

8           20. Defendant KMA Merchant Services, LLC (“KMA”) is a New Jersey  
9 limited liability company with its principal place of business at 714 N. 74<sup>th</sup> Street,  
10 Scottsdale, Arizona 85257. At all times material to this Complaint, KMA acted as an ISO  
11 sales agent for EPS, and referred merchants to EPS for underwriting approval and  
12 payment processing services. KMA also acted as a merchant and processed its own  
13 merchant transactions using EPS’s ISO services. KMA transacts or has transacted  
14 business in this district and throughout the United States.  
15  
16

17           21. Defendants EP Services, EPSA, and KMA used various dba names  
18 interchangeably, including EPS, EPSA, EPS-America, EPS of Arizona, EPS AZ, KMA,  
19 KMA Merchant Services, KMA Svcs, and Merchant Services. Emails sent by KMA  
20 indicate that KMA was the “customer service at EPS-america.net.”  
21  
22

23           22. Defendant Dynasty Merchants, LLC (“Dynasty”) is an Arizona limited  
24 liability company with its principal place of business at 731 S. Arizona Ave., Chandler,  
25 Arizona 85225. At all times material to this Complaint, Dynasty acted as a merchant and  
26 processed its own merchant transactions using EPS’s ISO services. Dynasty transacts or  
27 has transacted business in this district and throughout the United States.  
28

1           23. Defendant Wigdore is the President of EP Services and a director of EPSA.  
2 Individually and as an officer of EP Services and EPSA, Wigdore acted as an ISO sales  
3 agent for EPS. At all times material to this Complaint, acting alone or in concert with  
4 others, he has formulated, directed, controlled, or participated in the acts and practices of  
5 EP Services, EPSA, and KMA, including the acts and practices set forth in this  
6 Complaint. Wigdore resides in this district, and transacts or has transacted business in  
7 this district and throughout the United States.  
8  
9

10           24. Defendant Abdelmesseheh, also known as Michael Stewart, is a director of  
11 EPSA and a managing member of KMA. Individually and as an officer of KMA and  
12 EPSA, Abdelmesseheh acted as an ISO sales agent for EPS. At all times material to this  
13 Complaint, acting alone or in concert with others, he has formulated, directed, controlled,  
14 or participated in the acts and practices of EP Services, EPSA, and KMA, including the  
15 acts and practices set forth in this Complaint. Abdelmesseheh resides in this district, and  
16 transacts or has transacted business in this district and throughout the United States.  
17  
18

19           25. Defendant Mihilli is an officer and member of Dynasty Merchants, LLC.  
20 Mihilli worked as a sub-agent for the ISO sales offices of Defendants Wigdore and  
21 Abdelmesseheh. At all times material to this Complaint, acting alone or in concert with  
22 others, he has formulated, directed, controlled, or participated in the acts and practices of  
23 Dynasty Merchants, LLC, including the acts and practices set forth in this Complaint.  
24 Mihilli resides in this district, and transacts or has transacted business in this district and  
25 throughout the United States.  
26  
27  
28

### **The EPS Defendants**

26. Defendant Electronic Payment Systems, LLC (“EPS”) is a Colorado limited liability company with its principal place of business at 6472 Quebec St., Englewood, Colorado 80111. EPS is an ISO and payment processor. Among other things, EPS markets payment processing services to merchants and arranges for merchants to obtain “merchant accounts” through which merchants can process credit card sales transactions. Using the services of payment processors, EPS processes credit card payments for merchants through EPS’s acquirer. EPS transacts or has transacted business in this district and throughout the United States.

27. Defendant Electronic Payment Transfer, LLC (“EPT”) is a Colorado limited liability company with its principal place of business at 6472 Quebec St., Englewood, Colorado 80111. EPT is closely affiliated with EPS, and uses the dba “Electronic Payment Systems.” EPT transacts or has transacted business in this district and throughout the United States.

28. Defendants EPS and EPT are controlled and owned by the same two principals, and are often referred to interchangeably as the same company. EPS is the outward-facing company to the public, while EPT is the entity that sometimes enters into the agreements that EPS holds with its acquirer and payment processors. This Complaint will refer to EPS and EPT collectively as “EPS.”

29. Defendant John Dorsey (“Dorsey”) is the CEO and co-owner of EPS and EPT. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, or participated in the acts and practices of EPS and

1 EPT, including the acts and practices set forth in this Complaint. Defendant Dorsey  
2 transacts or has transacted business in this district and throughout the United States.

3 30. Defendant Thomas McCann (“McCann”) is the Managing Member and co-  
4 owner of EPS and EPT. At all times material to this Complaint, acting alone or in concert  
5 with others, he has formulated, directed, controlled, or participated in the acts and  
6 practices of EPS and EPT, including the acts and practices set forth in this Complaint.  
7 Defendant McCann transacts or has transacted business in this district and throughout the  
8 United States.  
9

10  
11 31. Defendant Michael Peterson (“Peterson”) is the Risk Manager of EPS. At  
12 all times material to this Complaint, acting alone or in concert with others, he has  
13 formulated, directed, controlled, or participated in the acts and practices of EPS,  
14 including the acts and practices set forth in this Complaint. Defendant Peterson transacts  
15 or has transacted business in this district and throughout the United States.  
16  
17

## 18 **COMMERCE**

19 32. At all times material to this Complaint, Defendants have maintained a  
20 substantial course of trade in or affecting commerce, as “commerce” is defined in Section  
21 4 of the FTC Act, 15 U.S.C. § 44.  
22

## 23 **THE DECEPTIVE MONEY NOW FUNDING SCAM**

24 33. From 2011 to 2013, the principals of MNF operated a deceptive  
25 telemarketing scam, charging thousands of consumers more than \$7 million for worthless  
26 business opportunities and related upsells. In one principal variation of the scam, MNF  
27  
28

1 telemarketers falsely told consumers they would earn income by referring small  
2 businesses seeking loans to MNF.

3 34. According to one sales pitch, in exchange for an upfront payment of \$299  
4 to \$499, purchasers of MNF's business opportunity would go into business with MNF  
5 and receive lucrative commissions each time MNF made a loan to a small business  
6 referred by the consumer.  
7

8 35. After consumers made the upfront payment, MNF telemarketers then  
9 further engaged in deceptive "upsells," and convinced consumers to pay thousands of  
10 dollars more for so-called "leads," *i.e.*, names and contact information for businesses in  
11 need of loans. MNF telemarketers falsely promised consumers that these leads would  
12 easily generate hundreds or thousands of dollars per month in income, and would result  
13 in huge returns on the consumers' investment in the business opportunity.  
14

15 36. In granting the FTC's motion for summary judgment, the court found that  
16 MNF was a multi-million dollar scheme to defraud consumers. The entire MNF sales  
17 pitch was a brazen scam. MNF was a total fraud, and not actually in the business of  
18 making loans to small businesses. Consumers never earned any of the promised income  
19 from the MNF business opportunities, and typically lost their investment, with losses  
20 ranging from a few hundred dollars to tens of thousands of dollars per consumer.  
21

22 37. The MNF scam operated through a web of interrelated companies,  
23 including "Rose Marketing." When consumer complaints about MNF's scam mounted,  
24 threatening exposure of the scam, the principals and employees behind MNF changed the  
25  
26  
27  
28

1 scheme's name and created new companies to continue operating the scam, under  
2 different and constantly changing names.

3 38. The FTC filed an action against MNF and its related and successor  
4 companies on August 5, 2013, alleging that the deceptive and fraudulent business  
5 opportunity scam violated the FTC Act, the Business Opportunity Rule, and the  
6 Telemarketing Sales Rule. FTC v. Money Now Funding, LLC, et al., CV 13-01583-PHX-  
7 ROS (D. Ariz. 2013). The complaint, which was amended on December 16, 2013,  
8 alleged, among other things, that MNF created fictitious companies supposedly owned by  
9 various MNF employees and applied for merchant accounts under these fictitious  
10 companies, and that MNF then used such merchant accounts to launder its credit card  
11 transactions.  
12

13 39. In 2015, the FTC settled with many of the defendants named in the MNF  
14 scam, obtaining court orders banning eighteen individual defendants from selling  
15 business or work-at-home opportunities. Also in 2015, the court granted the FTC's  
16 motion for summary judgment against certain MNF defendants, and entered default  
17 judgments against the remaining MNF defendants, resulting in the entry of permanent  
18 injunctions and monetary judgments. In 2016, the Arizona Attorney General's office  
19 brought criminal charges against four individuals involved in the MNF scam. As of  
20 January 25, 2017, all four had entered guilty pleas, with the lead defendant agreeing to a  
21 five-year prison term.  
22  
23  
24  
25  
26  
27  
28

## BACKGROUND ON CREDIT CARD LAUNDERING

40. In order to accept credit card payments from consumers, a merchant must establish a “merchant account” with a merchant acquiring bank (as noted above, also referred to as an “acquirer”). A merchant account is a type of account that allows businesses to process consumer purchases by a credit or debit card.

41. The acquirer is the entity that has access to the credit card associations (such as Mastercard and VISA), and through which merchant accounts are established. Without a merchant account obtained through an acquirer, merchants are unable to process consumer credit or debit card sales transactions.

42. Acquirers commonly enter into contracts with ISOs, who solicit and sign up merchants for merchant accounts with the acquirer. In some cases, ISOs engage in the screening and underwriting of prospective merchants, operate the acquirer’s merchant processing program (directly or through the services of third party processors), and monitor the merchants’ transactions.

43. To market the ISO’s processing services, ISOs often use ISO “sales agents,” and persons working under these sales agents (called “sub-ISOs” or “sub-agents”), who solicit and refer prospective clients to the ISO for the ISO’s underwriting approval.

44. The credit card associations (“card networks”), such as VISA and Mastercard, require all participants in their networks, including the acquirers and their registered ISOs, to comply with detailed rules governing the use of the card networks. These rules include screening and underwriting merchants to ensure that they are

1 legitimate bona fide businesses, and to screen out merchants engaged in potentially  
2 fraudulent or illegal practices. The rules also prohibit the practice of credit card  
3 laundering.  
4

5 45. Merchants that pose a greater risk of fraud or financial loss to the ISO,  
6 acquirer and card networks may be denied merchant accounts. For example, the ISO or  
7 acquirer may be concerned that the merchant is engaged in deceptive marketing, illegal  
8 activity or will generate excessive rates of transactions returned by consumers  
9 (“chargebacks”).  
10

11 46. Consumers initiate “chargebacks” when they dispute credit card charges by  
12 contacting their “issuing bank,” which is the bank that issued the credit card to the  
13 consumer. When a consumer successfully disputes the charge, the consumer’s issuing  
14 bank credits the consumer’s credit card for the disputed amount, and then recovers the  
15 chargeback amount from the acquirer (the merchant’s bank). The acquirer, in turn,  
16 collects the chargeback amount from the merchant, either directly or through its ISO or  
17 payment processor.  
18  
19

20 47. In order to detect and prevent illegal, fraudulent or unauthorized merchant  
21 activity, the card networks operate various chargeback monitoring and fraud monitoring  
22 programs. For example, if a merchant generates excessive levels of chargebacks that  
23 trigger the thresholds set under VISA’s chargeback monitoring program, the merchant is  
24 subject to additional monitoring requirements and, in some cases, penalties and  
25 termination.  
26  
27  
28



1           48. In recent years, credit card laundering has become a common practice of  
2 fraudulent merchants who cannot meet a bank's underwriting criteria or who cannot  
3 obtain merchant accounts under their own names (whether because of excessive  
4 chargebacks, complaints, or other signs of illegal activity).

5  
6           49. Even when the fraudulent merchant can qualify for a merchant account, it  
7 often engages in laundering as a way to conceal its true identity from consumers, the  
8 acquirer, the card networks, and law enforcement agencies.

9  
10          50. To conceal their identities, fraudulent merchants often create shell  
11 companies to act as fronts, and apply for merchant accounts under these shell companies.  
12 Once the merchant accounts are approved, the fraudulent merchant then launders its own  
13 transactions through the shell company's merchant accounts.

14  
15          51. Fraudulent merchants often generate excessive rates of "chargebacks" from  
16 consumers who dispute the credit card charges. To avoid triggering the card networks'  
17 chargeback monitoring programs and attracting the scrutiny of the acquirer, fraudulent  
18 merchants often spread out their sales transaction volume across multiple merchant  
19 accounts—a practice commonly referred to as "load balancing."

20  
21          52. Because the VISA and Mastercard chargeback monitoring programs apply  
22 only to merchants with at least 100 chargeback transactions per month, fraudulent  
23 merchants can manipulate the system and avoid chargeback monitoring by spreading  
24 their transactions across multiple merchant accounts and ensuring that no single account  
25 has more than 100 chargebacks per month. They can also avoid triggering the monitoring  
26  
27  
28

1 programs by simply processing for short time periods, such as for a few weeks, that fall  
 2 below the monitoring programs' time thresholds.

3 53. In addition to evading the card networks' merchant monitoring programs,  
 4 fraudulent merchants sometimes spread their transactions across multiple merchant  
 5 accounts in order to circumvent the underwriting requirements or monitoring programs of  
 6 the ISO's acquirer. For example, if the acquirer's underwriting rules are more lenient for  
 7 merchants with lower projected sales volume, fraudulent merchants can artificially lower  
 8 the merchant's projected sales volume by applying for numerous low-volume merchant  
 9 accounts in the names of fictitious companies, thereby obtaining the acquirer's  
 10 underwriting approval that the merchant otherwise would not be able to obtain.  
 11

12 54. By spreading out merchant transactions across numerous and constantly  
 13 changing fraudulent merchant accounts over short time periods, fraudulent merchants and  
 14 unscrupulous ISOs can cause an enormous amount of economic harm to consumers,  
 15 before their transactions are detected or terminated by the ISO's acquirer or the card  
 16 networks.  
 17

## 18 **DEFENDANTS' BUSINESS ACTIVITIES**

### 19 **The KMA-Wigdore Defendants Engaged In a Scheme 20 To Launder Credit Card Payments For the MNF Scam**

21 *The KMA-Wigdore Defendants' Acts Directly Caused The Laundering Of  
 22 MNF Transactions Through Numerous Fictitious Companies' Merchant Accounts*

23 55. The MNF scam, in which consumer-victims were persuaded to make  
 24 purchases over the telephone, relied on MNF having the ability to accept victim funds via  
 25 credit and debit cards without raising fraud alerts. To conceal its identity and to prevent  
 26

1 the acquirer and card networks from scrutinizing and terminating its merchant account,  
2 MNF engaged in a scheme with the KMA-Wigdore Defendants to apply for a large  
3 number of fraudulent merchant accounts, each under a different fictitious name, through  
4 which MNF could launder charges to consumers' credit or debit card accounts.  
5

6 56. As part of this scheme, MNF created numerous fictitious companies, each  
7 using the name of a MNF principal or employee as the straw owner or purported  
8 principal of the company. These phony companies did not engage in any actual business.  
9 Thus, for example, one fictitious company was called "D&D Marketing," the supposed  
10 owner of which was actually an MNF employee with the initials "D.D." When consumer-  
11 victims signed up for the MNF business opportunity and made a payment, their credit  
12 card statements would show a charge made by a company they had never heard of, such  
13 as "D&D Marketing," rather than Money Now Funding.  
14

15 57. During the period from May 2012 to November 2012, Defendant Wigdore,  
16 as an ISO sales agent, submitted phony merchant applications on behalf of 23 fictitious  
17 companies to EPS for EPS's underwriting approval. These 23 fictitious companies  
18 created by the MNF scam include: Zoom Docs; Doc Assistant; US Legal Docs; D&D  
19 Marketing; JJB Marketing; A&D Marketing; Miller Marketing; Ronn Hobbs &  
20 Associates; Global One Media; DePaola Marketing; Wisdom Management Group;  
21 National Marketing Group; Rose Marketing; Green Merchant Marketing; KT  
22 Advertising; V&R Marketing; BC Media Solutions; Elite Marketing Strategies; AJ  
23 Marketing; Midwarren Enterprises; Montgomery Marketing; McIntyre Marketing; and  
24 LJT Marketing ("2012 MNF Fictitious Companies").  
25  
26  
27  
28

1           58. When submitting the 23 phony applications, Wigdore used his own  
2 individual name as the sales agent, but did not list himself as acting under Electronic  
3 Payment Services, Inc. (the company Wigdore controlled that was also acting as an ISO  
4 sales agent for EPS). Instead he listed himself as acting under KMA Merchant Services  
5 (the company ostensibly controlled by Defendant Abdelmesseh that had a contractual  
6 agreement with EPS to act as EPS's sales agent).  
7

8           59. When applying for a merchant account, merchants often submit with the  
9 application a copy of a voided check drawn on their business bank account, with the  
10 understanding that credit card sales revenues will be transferred into this account.  
11

12           60. For each of the 23 fraudulent merchant applications, Wigdore attached a  
13 falsified voided (or preprinted) check that purported to reflect the existence of a business  
14 bank account in the name of that fictitious company. Each check had been doctored to  
15 reflect an account holder, *i.e.*, the fictitious company, that was not the true account holder  
16 for that account number. The account number printed on the bottom of each check  
17 corresponded with one of 23 different bank accounts at J.P. Morgan Chase Bank  
18 ("Chase"), each in the name of Defendant Dynasty Merchants, LLC, a company  
19 controlled by Defendant Mihilli.  
20

21           61. The 23 bank accounts at Chase ("Dynasty Chase Accounts") were set up by  
22 Wigdore's associate, Defendant Mihilli, who worked as a sub-agent under the KMA sales  
23 office of Defendants Wigdore and Abdelmesseh.  
24  
25  
26  
27  
28

1           62. After receiving the fraudulent applications from Wigdore, EPS approved all  
2       23 applications, set up merchant accounts for each fictitious company, and immediately  
3       began processing for these accounts through EPS's acquirer, Merrick Bank ("Merrick").  
4

5           63. When MNF transactions were processed through the 23 fraudulent  
6       merchant accounts in the names of the fictitious companies, the sales revenues from these  
7       transactions were automatically transferred into the 23 Dynasty Chase Accounts, and  
8       subsequently transferred into a "Master Account" at the same bank, also held in the name  
9       of Dynasty.  
10

11          64. From the Dynasty "Master Account," funds were divided up and eventually  
12       paid to Defendant EP Services (a company controlled by Wigdore, and an alias of KMA),  
13       companies affiliated with the MNF scam (*e.g.*, Rose Marketing), and individually to  
14       Defendants Abdelmesseah and Mihilli.  
15

16          65. The scheme allowed MNF to obtain merchant accounts based on false  
17       information in the merchant applications. Specifically, each merchant application  
18       contained the following false information: (1) the name of the fictitious company was  
19       listed as the applicant, when the true applicant was the principal(s) of the MNF scam; (2)  
20       the name of the straw owner was listed as the owner of the business, when the true owner  
21       was the owner(s) of the MNF scam; and (3) the fictitious company was listed as the  
22       account holder of the merchant bank account, when the true account holder was Dynasty  
23       Merchants, LLC.  
24  
25

26          66. The structure of the laundering scheme—in which revenues from the MNF  
27       sales transactions were processed through fraudulent merchant accounts in the names of  
28

1 the 23 fictitious companies and were ultimately funneled to both the MNF scam's  
2 principals and to bank accounts controlled by Defendants Wigdore, Abdelmessehe and  
3 Mihilli—establishes one aspect of the central role played by the KMA-Wigdore  
4 Defendants in the scheme. The KMA-Wigdore Defendants' acts in submitting fraudulent  
5 applications for the 2012 MNF Fictitious Companies directly caused the laundering of  
6 MNF transactions through these fictitious companies' merchant accounts.  
7

8  
9 67. In 2013, the principals, employees and associates of MNF changed the  
10 MNF fraudulent scheme's name, and continued operating the same scam through newly  
11 created companies and aliases (i.e. "Affinity Technologies, "Green Merchant Funding,"  
12 "Nationwide Lending"), and using numerous new fictitious company names ("2013 MNF  
13 Fictitious Companies"). The KMA-Wigdore Defendants submitted to EPS phony  
14 applications for these 2013 MNF Fictitious Companies. In turn, EPS approved the phony  
15 applications, opened merchant accounts for the 2013 MNF Fictitious Companies at  
16 Merrick, and continued processing transactions for the MNF scam through these  
17 fraudulent merchant accounts.  
18

19  
20 68. In addition to laundering MNF transactions through the 2012 MNF  
21 Fictitious Companies and the 2013 MNF Fictitious Companies (collectively, "MNF  
22 Fictitious Companies"), Defendants Abdelmessehe and Mihilli also participated directly in  
23 the MNF scam by laundering MNF transactions through their own merchant accounts.  
24  
25  
26  
27  
28

*Defendants Abdelmesseih And KMA Laundered MNF  
Transactions Through KMA's Own Merchant Accounts*

69. In addition to acting as EPS's ISO sales agent under KMA, Defendant Abdelmesseih also purported to operate his own independent businesses (called KMA Leads, KMA Merchant Marketing, and KMA Merchant Services) that supposedly offered "advertising/marketing services" and "merchant services" to consumers.

70. EPS approved and helped open merchant accounts at Merrick for these three supposed KMA businesses. Between October 2010 and May 2012, EPS processed more than \$1,384,500 in transactions for the three KMA merchant accounts combined.

71. At least two of KMA's merchant accounts were used to launder MNF sales transactions. In other words, when MNF victims were duped into buying leads or making other payments as part of the MNF scam, some of them incurred credit card charges in the name of one of the "KMA" businesses.

*Defendant Mihilli Laundered MNF Transactions  
Through Mihilli's Own Dynasty Merchant Account*

72. In addition to working as a sub-agent under the ISO sales office of Defendants Wigdore and Abdelmesseih, Defendant Mihilli also purported to operate his own independent business, Dynasty Merchants, LLC (sometimes using the dba "Dynasty Marketing"), that supposedly offered "marketing services" to consumers.

73. EPS approved and helped open a merchant account in the name of "Dynasty Marketing" at Merrick. Between May 2012 and September 2012, EPS processed more than \$228,162 in transactions through this merchant account. In some cases, MNF transactions were processed through this merchant account. This meant that

1 when MNF victims were duped into buying leads or making other payments as part of the  
 2 MNF scam, some of them incurred credit card charges in the name of “Dynasty  
 3 Marketing.”

4  
 5 **EPS Directly Caused the Laundering of MNF Transactions Through Numerous**  
 6 **Merchant Accounts Created In The Names of Other Companies**

7 74. Throughout 2012 and 2013, EPS directly caused consumers’ credit or debit  
 8 card accounts to be charged by MNF’s deceptive telemarketing scam by underwriting and  
 9 approving the MNF Fictitious Companies and the Mihilli and Abdelmesseh businesses  
 10 for processing, establishing merchant accounts for these entities with Merrick, and  
 11 processing for these merchant accounts.  
 12

13 75. Without the ISO and processing services provided by EPS, the MNF scam  
 14 could not have obtained the fraudulent merchant accounts established at Merrick, through  
 15 which their credit card transactions were processed.  
 16

17 ***EPS Touted Itself as a Processor for “High Risk” Merchants and Used Wigdore as a***  
 18 ***Sales Agent Despite His Criminal History***

19 76. In order to solicit and locate prospective merchants, EPS operated an ISO  
 20 sales program under which it used ISO “sales agents” to market EPS’s services and to  
 21 refer merchant applications to EPS for underwriting approval. EPS actively sought to  
 22 recruit sales agents, and entered into independent contractor agreements (“Marketing  
 23 Agreements”) with these agents.  
 24

25 77. According to statements made by EPS in court filings in July 2016 (*see*  
 26 *Mot. To Quash* (ECF No. 9), Electronic Payment Transfer, LLC v. Federal Trade  
 27 Commission and Citywide Banks, No. CV-01653-RBJ (D. Colo. July 11, 2016)), EPS’s  
 28



1 relationship with Wigdore dated back to approximately 2004. This relationship continued  
2 while Wigdore served a 57-month sentence on a federal fraud conviction from 2006 to  
3 2009; during this period Wigdore's wife, Sandy Wigdore, continued acting as an ISO  
4 sales agent for EPS.  
5

6 78. EPS's principal, Defendant Thomas McCann, was fully aware of  
7 Wigdore's criminal history, but chose to continue using Wigdore as EPS's sales agent.  
8 On August 6, 2008, Sandy Wigdore handwrote the following comments on a fax cover  
9 sheet that accompanied a Marketing Agreement faxed to EPS:  
10

11 P.S. Let me know what Tom [Defendant Thomas McCann] thinks – they  
12 (Probation dept.) start coming around in a month or so to ask me questions  
13 about Jay working and maybe call you guys to confirm. – Thank you so  
14 much.

15 79. Defendant Thomas McCann had a longstanding personal relationship with  
16 Wigdore, as reflected in various email messages from 2010 and 2011, such as the  
17 message "Please call Jay Wigdore on his cell. He says he has some gossip for you" or  
18 "Jay Wigdore called while you were at lunch. He said that if you were coming to town he  
19 would like to take you to dinner and introduce you to Les."  
20

21 80. McCann's and Dorsey's interest in using Wigdore as EPS's sales agent was  
22 not surprising. EPS has held itself out as a processor for "High Risk" businesses that have  
23 difficulty finding banks willing to accept their business. As recently as November 2015,  
24 EPS's website touted the fact that it had a "98% Approval Rate" for merchants who  
25 applied for its credit card processing services, as compared to its competitors who had a  
26 "60% Approval Rate."  
27  
28

1           81.    EPS’s website actively sought out the business of “High Risk Merchants,”  
2 and offered to help merchants set up “offshore merchant accounts.” The website stated:

3           Is your business having trouble getting approved for traditional merchant service  
4 accounts? Do you need a High Risk Merchant Account? . . . We can get your High  
5 Risk merchant account approved in a quick and professional manner. When US  
6 domestic banks won’t accept a High Risk Merchant, EPS has special partnerships  
with international banks overseas to set up an offshore merchant account with.

7           82.    As an ISO for Merrick, EPS was contractually required to comply with  
8 Merrick’s underwriting rules for screening merchants, which included strict guidelines  
9 designed to verify the identity of the merchant and the legitimacy of the merchant’s  
10 business, and to screen out merchants potentially engaged in fraud. Indeed, Merrick’s  
11 policy required EPS to verify “that each merchant is a bona fide business and that the  
12 transactions of such merchant will reflect bona fide business between the merchant and  
13 the cardholder, and will not violate any applicable provision of law.” EPS was also  
14 required to monitor its merchants’ transactions, update merchant information in the  
15 merchant database, and ensure that its merchants complied with the card networks’ rules  
16 and various fraud monitoring programs. As a registered ISO with VISA (through  
17 Merrick), EPS also was required to comply with VISA’s rules and regulations.  
18  
19  
20  
21

22           83.    However, rather than verify its merchants’ identities, EPS opened merchant  
23 accounts in the names of numerous fictitious companies for the same underlying  
24 merchant, and thereby falsely represented the true identity of the fictitious companies. In  
25 concealing the true identity of the fictitious companies, EPS also evaded the various card  
26 network fraud and chargeback monitoring programs that were designed to detect and  
27 prevent fraudulent activity.  
28

1           84. The chronology of EPS's involvement in the MNF scam's credit card  
2 laundering shows that EPS: (a) ignored obvious warning signs of fraud, including the  
3 likely presence of credit card laundering, (b) concealed from Merrick (the acquirer) and  
4 the card networks the true identity and nature of the MNF Fictitious Companies, and (c)  
5 made every effort to continue processing for the MNF Fictitious Companies, and other  
6 merchants related to the KMA-Wigdore Defendants, even after Merrick noticed signs of  
7 fraud and instructed EPS to stop.  
8  
9

10                   ***December 2011: Merrick Rejects KMA Merchant Account***

11           85. EPS processed merchant transactions through three merchant accounts it  
12 had opened for Defendant KMA. As early as December 2011, Merrick declined a  
13 merchant application that EPS submitted for one of KMA's merchant accounts, under the  
14 name "KMA Leads."  
15

16                   ***March 2012 - May 2012: Merrick Notified EPS That a KMA Merchant Account Had***  
17                   ***an Unacceptably High Chargeback Ratio, and Appeared To Be "Load Balancing"***

18           86. Even though Merrick had declined one KMA merchant account ("KMA  
19 Leads"), EPS continued processing for another KMA merchant account—"KMA  
20 Merchant Services." That account presented a range of problems from March 2012  
21 through May 2012, detailed below, leading Merrick to request EPS to terminate the  
22 account.  
23  
24

- 25           a) On March 20, 2012, Merrick's Risk Management department emailed  
26 Defendant Peterson, alerting him that the KMA Merchant Services  
27  
28

1 merchant account had triggered Mastercard's fraud monitoring program,  
2 and requesting additional merchant information.

- 3  
4 b) On April 10, 2012, Merrick again emailed Peterson, notifying him that  
5 Mastercard was requesting additional information about KMA, including  
6 details "as to what fraud control measures in place at the merchant  
7 location...."
- 8  
9 c) On April 17, 2012, Merrick's Risk Manager emailed Peterson regarding the  
10 KMA merchant account, this time alerting him to five consumer  
11 chargeback requests that indicated "Services not provided or merchandise  
12 not received" as the reason for the chargeback, and an additional  
13 chargeback complaint regarding a related KMA account that indicated  
14 "Fraudulent transaction no cardholder authorization."
- 15  
16 d) On April 18, 2012, Merrick's Risk Manager emailed Peterson regarding  
17 KMA's 15.6% chargeback rate, stating: "This account is processing well  
18 over the assigned volumes and their chargeback ratio is unacceptable ...."
- 19  
20 e) On May 11, 2012, Merrick's Risk Manager again emailed Peterson  
21 regarding KMA:

22  
23 I have reviewed in detail your chargeback reduction plan  
24 for KMA. The business was incorporated in 2011 and I  
25 am inclined to not believe that they are unfamiliar with  
26 how to run their business. It is ironic that as soon as they  
27 came onboard with EPS their volume skyrocketed and  
28 they blew through the volume caps UW [underwriting]  
had in place . . . Another concern is the amount of  
chargebacks and the reason codes for them (services not  
provided) ... The merchant's business model as

described in the plan is unclear and sounds a lot like they are conducting lead generation, which Merrick was not comfortable with processing for in the first place ....

f) Merrick's email went on to express the opinion that KMA was engaging in load balancing, and instructed EPS to terminate the KMA accounts if KMA could not succeed in lowering its chargeback levels to an acceptable level:

The other KMA account MID # xx 5830 also has been processing well over their capped volumes . . . and has unacceptable chargeback ratios. I personally believe that they are load-balancing and processing for both the account that was declined and the one we are discussing.... [Emphasis added]

87. As discussed in Paragraphs 51-53 above, "load balancing" refers to the practice of spreading out a merchant's transactions across numerous merchant accounts in order to limit the volume of transactions processed through any one single merchant account, and thereby to avoid triggering the chargeback thresholds for the acquirer's or card networks' chargeback monitoring programs.

88. As a result of Merrick's instructions to terminate KMA's merchant accounts, EPS stopped processing new transactions for KMA's merchant accounts around May 2012. However, EPS continued to approve merchant account applications submitted by KMA (acting in its capacity as EPS's sales agent).

***May 2012 - June 2012: Merrick Rejected Merchant Applications Submitted By EPS Because They Appeared to Be KMA-Related***

89. Even after Merrick instructed EPS to terminate the KMA merchant accounts of KMA due to concerns regarding load balancing, fraud, and excessive chargebacks, EPS and its principals nonetheless continued approving new merchant

1 applications submitted to it by the same entity, KMA (this time acting in its capacity as  
2 EPS's sales agent, rather than as a client merchant itself). EPS chose not to inform  
3 Merrick that KMA was the sales agent for these new merchant applications. However,  
4 when Merrick would discover a KMA connection, Merrick would decline the application.  
5

6 90. On May 24, 2012, Merrick informed Defendant Peterson that it had  
7 declined three merchant applications because the alleged principals of these merchants all  
8 shared the same email address as the principal of the merchant KMA. Merrick noted that  
9 the three declined merchants "have principal email addresses with the alias being at  
10 kmamarketingsvcs.com – KMA had chargeback issues with us in the past."  
11

12 91. One week later, on May 31, 2012, Merrick declined yet another application,  
13 again informing Peterson that the merchant "also appears to be linked to KMA Marketing  
14 which has had chargeback issues with us."  
15

16 92. Two weeks later, on June 14, 2012, Merrick declined four more merchant  
17 applications, this time highlighting the fact that all four applications had been referred to  
18 EPS by the same sales agent ("sales channel 2088," a sales office number that EPS had  
19 assigned to KMA, acting as its sales agent), and that the merchants were all "home-based  
20 marketing companies," a business model that Merrick had indicated it was not  
21 comfortable with.  
22

23 93. Despite these rejections and Merrick's repeatedly-stated desire not to do  
24 business with companies linked to the merchant KMA, Peterson continued to submit new  
25 merchant applications to Merrick that had been referred by EPS's "sales agent" KMA,  
26  
27  
28

without informing Merrick that KMA was the underlying sales agent who had referred those applications to EPS.

***May 2012 - November 2012: EPS Approved The 23 Fraudulent  
MNF Merchant Applications Provided By Sales Agent KMA  
Despite Multiple Suspicious Red Flags***

94. From May to November 2012, Defendant Wigdore submitted 23 merchant applications on behalf of the 2012 MNF Fictitious Companies to EPS. Each application indicated that the sales agent was “Jay Wigdore” of ISO sales office “2088.” As noted above, this was the number EPS had assigned to its sales agent KMA, although on their face the applications did not mention KMA directly. In addition to the fact that the applications were referred by the sales agent KMA, an entity whose own business (as an EPS client merchant) Merrick had repeatedly rejected due to concerns about fraud, these applications from 23 supposedly different merchants appeared virtually identical and contained numerous suspicious red flags, as described below. EPS approved them all.

- a) Almost all the merchants were located in the Phoenix, Arizona area. The “business description” provided for most of the merchants was extremely vague, almost always identical (*i.e.* “marketing and advertising”), and provided no specific description of the product or service being sold.
- b) The 23 supposedly separate merchants attached facially suspect checks that appeared almost identical in form. Each of the attached doctored checks was drawn on Chase bank and had the same bank routing number, indicating the same bank branch. Almost all of them bore the same check number—“1001.” The fact that 23 supposedly different merchants all

1           purported to hold accounts at the same bank branch and submitted virtually  
2           identical checks (almost always bearing the same check number) was a  
3           glaring indicator that they were likely related to each other or to the same  
4           underlying merchant. Despite these red flags, EPS did not even bother to  
5           verify the legitimacy of the 23 bank accounts at Chase.

6  
7           c) During the initial underwriting stage, EPS obtained credit reports for each  
8           of the 23 fictitious companies. For most of the merchants, the credit reports  
9           indicated that the principals or owners of the businesses had low credit  
10          scores, poor credit ratings, and owed substantial outstanding debts, raising  
11          obvious questions about the financial health of the merchants and the nature  
12          of their businesses. EPS nonetheless approved the 2012 MNF Fictitious  
13          Companies, without seeking to obtain additional information about the  
14          businesses or their financial viability.

15  
16  
17          d) Although Merrick's underwriting policy required EPS to obtain and  
18          evaluate samples of all relevant merchant marketing materials and  
19          telemarketing scripts, the 23 merchant applications failed to include copies  
20          of the merchants' marketing materials.

21  
22          e) Merrick's policy further required EPS to obtain screen prints of the relevant  
23          web pages of the merchant's website for "high risk" merchants such as  
24          telemarketers; however, for at least six merchant applications, the "Initial  
25          Risk Evaluation" conducted by EPS's employee specifically noted that the  
26          merchant did not have a valid merchant website.  
27  
28



1 f) In the case of at least five merchant applications, the address listed on the  
 2 credit report did not match the address listed for the merchant on the  
 3 merchant application.

4 g) For at least five of the merchant applications, an attached Application  
 5 Addendum form stated that “Jay Wigdore” was a co-owner or co-officer of  
 6 the alleged merchant, in addition to another co-owner or co-officer whose  
 7 name was listed on the application form.

8 h) In the case of five merchants, the merchant’s business bank account was  
 9 listed on the application as “Comerica Bank,” even though the checks  
 10 attached to the applications indicated that the merchant’s bank was Chase  
 11 Bank, and not Comerica Bank. Despite this obvious inconsistency, EPS  
 12 nonetheless approved these applications.

13 95. Had EPS sought to verify the legitimacy of the 23 merchant bank accounts,  
 14 it would have discovered that the true account holder for each of the 23 Chase bank  
 15 accounts was not the fictitious company whose name was printed on the check and listed  
 16 on the merchant application, but a different company: Dynasty Merchants, LLC.

17  
 18  
 19  
 20  
 21 ***The EPS Defendants Concealed the Fact That the Fictitious Companies Were High-  
 22 Risk Telemarketers, Thereby Shielding Them From Enhanced Scrutiny By Merrick or  
 23 VISA***

24 96. Many of the merchant applications for the MNF Fictitious Companies  
 25 submitted by Wigdore contained clear indications that the merchants were engaged in  
 26 telemarketing. For example, a section on the application form entitled “Merchant  
 27 Product/Service Profile” asked “How is the Product or Service Ordered or Purchased  
 28

1 (mail order, catalog, over the phone, in person, etc.).” The merchant applications  
2 contained the handwritten response “over the phone,” indicating telemarketing.

3 97. Because telemarketers pose a higher risk of fraud, VISA rules require  
4 telemarketers to be classified and coded as “High Brand Risk Merchants.” VISA rules  
5 further require that the correct “Merchant Classification Code” (or “MCC”) be assigned  
6 to all merchants. The MCC numbers 5966 and 5967 are used to indicate inbound and  
7 outbound telemarketers, which are “High Brand Risk Merchants.”  
8

9  
10 98. VISA imposes heightened monitoring requirements for all merchants that  
11 are coded as “High Brand Risk Merchants,” including merchants engaged in  
12 telemarketing. These monitoring requirements are designed to detect and prevent  
13 merchants from processing fraudulent or illegal credit card transactions through VISA’s  
14 network.  
15

16 99. Even though the merchant applications for many of the MNF Fictitious  
17 Companies indicated that these entities were engaged in telemarketing, EPS concealed  
18 this fact by failing to assign to these entities the correct MCC number required for  
19 telemarketers. Instead, EPS entered MCC number 7311, which simply refers to  
20 “advertising services.”  
21

22  
23 100. By not coding the MNF Fictitious Companies as telemarketers and  
24 concealing this fact, EPS was able to avoid placing these merchants under the heightened  
25 monitoring program required by VISA for “High Brand Risk Merchants.”  
26

27 101. Also, Merrick’s underwriting policy and rules prohibited EPS from  
28 processing for telemarketers (and other categories of merchants deemed by EPS to be

1 “high risk”), prior to obtaining Merrick’s approval. Even though the applications  
2 indicated that many of the MNF Fictitious Companies were engaged in telemarketing,  
3 EPS began processing for these entities prior to obtaining Merrick’s approval, in direct  
4 violation of Merrick’s rules.  
5

6 ***May 2012 - July 2012: EPS Processed For At Least 11 Fictitious Companies Declined***  
7 ***By Merrick, In Some Cases For More Than Two Months After They Had Been***  
8 ***Declined***

9 102. Not only did EPS begin processing for MNF’s fictitious companies before  
10 these companies were approved by Merrick, EPS also *began processing* for certain MNF  
11 fictitious companies *even after* Merrick already had declined the applications for these  
12 same fictitious companies.  
13

14 103. Between May 2012 and June 2012, Merrick declined 11 fraudulent  
15 merchant applications approved and submitted by EPS on behalf of the 2012 MNF  
16 Fictitious Companies. EPS nonetheless continued processing for these fictitious  
17 companies, in some cases for more than two months after they had been declined by  
18 Merrick.  
19

20 104. By the end of June 2012, EPS had processed more than \$573,000 in  
21 transactions for the 11 declined fictitious companies, for time periods ranging from just  
22 two weeks to eight weeks per merchant—short time periods that fall below VISA’s  
23 chargeback monitoring program thresholds.  
24

25 105. Below is a list of the 11 fictitious companies declined by Merrick, the time  
26 periods EPS processed for each company, and the amount of transactions processed  
27 through each merchant account:  
28

<u>MNF Fictitious Company</u>	<u>Time Period Processed</u>	<u>Amount Processed</u>
JJB Marketing	4 weeks	\$ 29,600
Miller Marketing	7 weeks	\$ 67,400
Ron Hobbs	5 weeks	\$ 32,100
National Marketing GP	4 weeks	\$ 52,500
Rose Marketing	5 weeks	\$ 50,247
Wisdom Management	6 weeks	\$ 64,000
D&D Marketing	6 weeks	\$ 80,400
DePaola Marketing	2 weeks	\$ 9,500
KT Advertising	8 weeks	\$115,050
V&R Marketing	7 weeks	\$145,100
Green Merchant	2 weeks	\$ 55,598

***July 2012 - September 2012: After Merrick Declined 11 Merchant Applications Submitted To EPS By Sales Agent Wigdore, EPS Approved and Forwarded to Merrick Seven New Fraudulent Applications Referred By the Same Sales Agent***

106. By the end of June 2012, Merrick had declined 11 applications referred to EPS by Wigdore. Between July 24, 2012 and September 5, 2012, EPS nonetheless approved and forwarded to Merrick seven additional fraudulent merchant applications (for seven of the 2012 MNF Fictitious Companies), each of which had been referred by Wigdore.

107. These seven new applications appeared suspiciously similar to the 11 applications previously declined by Merrick. They attached the same facially suspect checks indicating that the merchants all banked at the same bank (“Chase”) and had the same routing number. Four applications indicated that the merchant’s bank was Comerica, even though they attached a “Chase” bank check. The credit report for one merchant (LJT Marketing) indicated an extremely poor credit score and a “past due amount” of \$144,904 owed by the merchant, while the credit report for another merchant (Midwarren Enterprises) showed a “past due amount” of \$24,344. The address listed on

1 the credit report for a third merchant (McIntyre Marketing) did not match the merchant  
2 address listed on the application. For four of the merchants, the initial risk review  
3 conducted by an EPS employee specifically noted that no marketing materials or web  
4 listings for the merchant had been submitted or found. (BC Media Solutions,  
5 Montgomery Marketing, McIntyre Marketing, LJT Marketing). Despite these obvious red  
6 flags, EPS nonetheless approved all seven applications.  
7

8  
9 108. As in the past, EPS processed for these seven new accounts for short time  
10 periods, typically ranging from three to seven weeks.

11 ***Consumer Chargebacks Indicated That Some of the Fictitious Company***  
12 ***Merchant Accounts Approved By EPS Were Used To Launder MNF Transactions***

13 109. Merrick's underwriting policy required EPS to monitor its client  
14 merchants' transactions "in order to detect unusual or unacceptable trends in such  
15 Merchant's processing activity," and to monitor its merchants' chargeback transactions  
16 and consumer inquiries relating to these chargeback transactions.  
17

18 110. EPS regularly monitored its merchants' chargeback transactions. Through  
19 the processing platforms provided by two payment processors, EPS had access to its  
20 merchants' chargeback transaction data, together with the consumer complaints that  
21 accompanied chargeback requests.  
22

23 111. Once EPS began processing for the 23 accounts set up for the 2012 MNF  
24 Fictitious Companies, these accounts began generating substantial chargebacks, many of  
25 which included "chargeback reason codes" indicating that the merchant's charges either  
26  
27  
28

1 were not authorized by the consumer, were fraudulent, or that the merchant failed to  
2 provide the goods or services as promised.

3 112. In some cases, the chargeback requests included consumer complaints and  
4 documentation clearly indicating that the merchant involved was “Money Now Funding,”  
5 and not the fictitious company whose name was on the merchant account—obvious  
6 evidence of credit card laundering.  
7

8 113. Despite having clear evidence of illegal credit card laundering through a  
9 KMA merchant account, EPS not only failed to stop doing business with KMA, but  
10 actively sought to protect KMA’s ability to continue laundering, as set forth below.

11 ***September 2012: EPS’s Risk Manager Knew That MNF Transactions Were Laundered***  
12 ***Through a KMA Merchant Account, and Directly Instructed KMA to Spread Out Its***  
13 ***Merchant’s Transactions Across Numerous Merchant Accounts***  
14

15 114. As EPS’s Risk Manager, Defendant Peterson oversaw EPS’s Risk  
16 Department, and closely interacted with EPS’ principals, Defendants Dorsey and  
17 McCann, and EPS’s Chief Operating Officer (“COO”).  
18

19 115. Peterson directly communicated with Defendants KMA and Abdelmesseh  
20 on a regular basis, and knew that KMA was acting as both EPS’s sales agent and a “client  
21 merchant” for whom EPS processed transactions. Peterson knew that MNF transactions  
22 were being laundered through at least one of KMA’s three merchant accounts, in the  
23 name KMA Merchant Services.  
24

25 116. On September 4, 2012, Peterson received an email from an EPS employee  
26 working directly under Peterson’s supervision. The email forwarded to Peterson a  
27 consumer’s chargeback dispute documentation for a “KMA Merchant Services”  
28

1 merchant account and stated: “all supporting documentation sent in to rebuttal dispute has  
2 ‘Rose Marketing, LLC’ plastered all over the paperwork.”

3 117. As discussed previously, Rose Marketing was one of the companies that  
4 sold MNF’s bogus business opportunity. The chargeback documents clearly indicated  
5 that the transactions for a company called “Rose Marketing” had been laundered through  
6 the KMA merchant account.  
7

8 118. Peterson immediately forwarded the email to “Mike Stewart” of KMA  
9 (Defendant Abdelmesseh), adding:  
10

11 Stewart, We cannot win pre-arb [prearbitration] with this  
12 documentation. We are going to have to let the cardholder win on  
13 this one as the argument against factoring is too great. Please review  
14 and advise.  
(Emphasis added.)

15 As noted above, the practice of credit card laundering is often referred to as  
16 “factoring.”  
17

18 119. Peterson also directly instructed Abdelmesseh, acting in his capacity as  
19 EPS’s sales agent, to spread out the transactions of KMA’s client merchant across  
20 multiple merchant accounts opened in the names of the fictitious companies.  
21

22 120. In a September 17, 2012 email to “Mike Stewart” of KMA (Defendant  
23 Abdelmesseh), Peterson wrote:

24 Stewart, Please see my notes below for the accounts that are on hold.  
25 We need to spread this out more, I am trying to cap each individual  
26 account in the \$30-\$40K range, so if you need to build a couple  
27 more accounts to reach your volume, please do so... [Emphasis  
28 added]

1           121. The referenced merchant accounts (“the accounts that are on hold”)  
2 included at least six of the 2012 MNF Fictitious Companies’ merchant accounts that EPS  
3 had opened and used to process MNF transactions.  
4

5           122. With respect to one of these merchant accounts, Peterson placed an explicit  
6 note: “On Hold – Pay out Tuesday – Do not put any more volume for the month through  
7 this one!”  
8

9           123. Because Merrick’s underwriting rules or monitoring practices were in part  
10 based on a merchant’s projected or actual sales volume, a fraudulent merchant might  
11 obtain Merrick’s approval or avoid Merrick’s scrutiny if it appeared to process a lower  
12 volume of transactions.  
13

14           124. By knowingly processing transactions for the same underlying merchant  
15 (that is, MNF) through multiple merchant accounts opened in the names of the fictitious  
16 companies, Peterson directly engaged in credit card laundering. He knowingly concealed  
17 the true identity of the merchant (MNF). Peterson also engaged in tactics to evade  
18 Merrick’s underwriting rules or monitoring practices and the card networks’ chargeback  
19 monitoring programs, by spreading out the MNF transactions across multiple merchant  
20 accounts in order to artificially lower the volume of sales and chargeback transactions  
21 processed through any single merchant account.  
22  
23

24           ***By February 2013, EPS Knew That The 2012 MNF Fictitious Companies Had***  
25           ***Changed Their Addresses to the Same Address, But Continued Using***  
26           ***Wigdore and Abdelmesseh As EPS’s Sales Agents***

27           125. In a February 21, 2013 email from KMA to an employee working in EPS’s  
28 Risk Department, KMA provided EPS a list of address changes for numerous client



1 merchants. The list clearly revealed that almost all of the 2012 MNF Fictitious  
2 Companies, and numerous additional merchants, had changed their addresses to the same  
3 address (three post office boxes located at the same address in Phoenix, Arizona), an  
4 obvious sign that these entities were related to the same underlying merchant.  
5

6 126. An EPS Risk Department employee forwarded the list of address changes  
7 to Defendant Peterson and wrote a note asking: “Why are all the addresses the same?”  
8

9 127. Despite knowing that numerous allegedly different merchants (including  
10 the 2012 MNF Fictitious Companies) referred by KMA/Wigdore shared the same  
11 business address, in addition to all the other red flags regarding fraudulent activity by  
12 Wigdore and Abdelmesseh, EPS decided to renew its sales agent relationship with them.  
13

14 ***March 2013: EPS Entered Into a Three-Year***  
15 ***Contract With Wigdore and Abdelmesseh***

16 128. In March 2013 EPS entered into a three-year “Marketing Agreement” with  
17 Defendant Electronic Payment Solutions of America, a company newly formed and  
18 jointly controlled by Wigdore and Abdelmesseh. EPS was so eager for business from  
19 Wigdore and Abdelmesseh that the contract included a provision requiring EPSA to  
20 submit all merchant applications to EPS on a “first right of refusal” basis, before referring  
21 merchants to other ISOs.  
22

23 ***Throughout 2013, EPS Continued Approving New Fraudulent Merchant Applications***  
24 ***and Opening Merchant Accounts for New Fictitious Companies of the MNF Scam***

25 129. By the end of 2012, Merrick had declined the vast majority of the 2012  
26 MNF Fictitious Companies. Despite this fact, throughout 2013, EPS continued accepting  
27 and approving merchant applications referred by Defendant Wigdore, using the “sales  
28

1 channel 2088.” These included phony merchant applications for the 2013 MNF Fictitious  
2 Companies.

3 130. Like the merchant applications for the 2012 MNF Fictitious Companies, the  
4 applications for the 2013 MNF Fictitious Companies contained obvious signs that the  
5 merchants likely were not legitimate businesses and were related to the same underlying  
6 merchant. For example, at least 14 supposedly different merchants purported to have  
7 bank accounts at the same bank branch, this time at a Wells Fargo Bank branch located in  
8 Mesa, Arizona.  
9

10  
11 131. The 2013 MNF Fictitious Companies included four fictitious entities  
12 controlled by Luke Rose, the principal of the MNF scam (S&P Marketing, CMH  
13 Marketing, CMT Marketing, GJ Financial). EPS processed at least \$98,300 in  
14 transactions for these four fictitious companies combined.  
15

16 132. The 2013 MNF Fictitious Companies also included fictitious companies  
17 controlled by managers of the MNF scam. One MNF manager, Cordell Bess, created a  
18 new fictitious company (Premier Online Marketing Strategies) to replace his previous  
19 fictitious company (JJB Marketing). In 2012, EPS had processed for JJB Marketing, until  
20 Merrick instructed EPS to terminate the company. The EPS employee who reviewed the  
21 application for Bess’s new company (Premier Online Marketing Strategies) specifically  
22 noted that EPS already had opened a “previous account” for the same underlying  
23 merchant. EPS nonetheless approved and processed \$62,795 in transactions for this new  
24 fictitious company.  
25  
26  
27  
28

1           133. A second MNF manager, Cynthia Miller, also known as “Cynthia Metcalf”  
2           and “Cynthia Wilson,” controlled at least 12 of the 2013 MNF Fictitious Companies  
3           (“Cynthia Miller Fictitious Entities”), including: Jones Advertising Options; A&P  
4           Marketing Solutions; Phipps Marketing Advantages; Rogers Online Marketing; Prompt  
5           Preparation Services; Independent Home Solutions and Marketing; Elite LLC Preparation  
6           Services; Quintin Marketing Strategies; Priority Online Marketing Strategies; JSK  
7           Marketing; SNC Advertising; Luczko Marketing and Advertising. EPS processed a total  
8           of \$1,666,003 in transactions through the 12 Cynthia Miller Fictitious Entities combined.  
9

10           134. Defendant Peterson was fully aware that the Cynthia Miller Fictitious  
11           Entities were in fact related to the same underlying merchant or individual. Indeed, in a  
12           spreadsheet attached to an email dated January 30, 2014 from Defendant Abdelmesse  
13           h (“Mike Stewart”) to Mike Peterson, Abdelmesse  
14           h listed the names of the 12 merchants,  
15           the name of the straw “owner” of each merchant, and indicated that all 12 merchants in  
16           fact belonged to the same “Group” that was associated with one individual – “Cynthia  
17           Wilson.”  
18

19           135. In 2013, EPS processed more than \$1,827,098 of MNF transactions for the  
20           2013 MNF Fictitious Companies combined.  
21

22  
23                           ***July 2013: EPS Falsely Represented To Law Enforcement***  
24                           ***That It Was No Longer Doing Business With KMA***

25           136. On July 18, 2013, the Oregon Department of Justice (“Oregon DOJ”)  
26           contacted EPS, informing it of an investigation into an entity possibly related to KMA for  
27           violations of the Telemarketing Sales Rule and other laws. The Oregon DOJ investigator  
28

1 asked EPS to clarify its relationship with KMA, and asked whether KMA was acting as a  
2 “satellite office” of EPS or as an EPS independent contractor.

3 137. In response to the Oregon DOJ’s inquiry, EPS’s COO sent an email, dated  
4 July 18, 2013, in which he falsely represented that EPS was no longer doing business  
5 with KMA: “As stated during our conversation yesterday, [EPS LLC] is a Colorado  
6 company.... Upon review of our information I see that we have done business in the past  
7 with a KMA Merchant Services LLC, an Arizona Corporate entity ... although they are  
8 no longer active.”

9 138. Contrary to EPS’ COO’s representations, EPS continued working with  
10 KMA, EPSA, Wigdore and Abdelmesseh long after the COO’s July 18, 2013 email. For  
11 example, in an August 21, 2013 email sent from Abdelmesseh (“Mike Stewart”) to  
12 Defendant McCann, Abdelmesseh stated:

13 We took this deal away from Powerpay. We sold it with no reserve. Please  
14 approve the deal for 75K to 100K monthly for each MID [referring to merchant  
15 accounts created, each with a “Merchant Identification” number] and we  
16 collectively will monitor the account. If a reserve is needed at a later time we can  
17 make that happen or shut off the account if it is not performing. We can get a lot  
18 of business from this customer via referral channel.

19 139. EPS continued approving and processing for new merchants submitted by  
20 KMA and Wigdore, and continued processing for merchants previously referred to EPS  
21 by KMA, through at least the end of December 2013.

### **EPS Knowingly Concealed the Identities of Additional Merchants**

140. EPS's company practice of knowingly processing for merchants whose true identities were concealed was not limited to the MNF Fictitious Companies. The practice applied to other merchants as well.

141. For example, in a September 17, 2013 email sent from EPS employee Chonda Pearson to an employee working in Wigdore's sales office, Pearson wrote: "Unfortunately this merchant has an open bankruptcy. We will be happy to process this deal with a new signer." Pearson's statement that the merchant circumvent Merrick's rules by simply finding a "new signer," is contrary to Merrick's underwriting policy that considered "any merchant that is currently in business bankruptcy" to be an "Unacceptable Merchant" for approval.

142. Similarly, in a May 20, 2013 email exchange between EPS employee Pearson and another employee in Wigdore's sales office, regarding a merchant called "M2M Gold," Pearson wrote: "This is the same signer—we need a different signer on the application." Pearson again reiterated this point two hours later, in a follow-up email, stating: "I spoke to Mike Peterson ... We cannot do anything with it until we have a different signer."

143. Peterson and Abdelmessehe kept close track of the various merchants whose true identities were concealed behind different company names. For example, a spreadsheet attached to the January 30, 2014 email from "Mike Stewart" to Peterson listed numerous companies that belonged to particular "Groups." Each Group was

1 associated with a single individual. For example, six “merchants” were identified as  
2 belonging to the “Group” associated with “Ryan Helms.” Five “merchants” were  
3 identified as belonging to the “Group” associated with “Andrew Chavez.” Six  
4 “merchants” were identified as belonging to the “Group” associated with “Ovi.”

5  
6 144. Of particular note, 17 “merchants” were identified as belonging to the  
7 “Group” associated with “Lance Himes.” Lance Himes was a former associate of MNF  
8 who had participated in the MNF scam.  
9

10 ***EPS Was Aware of Complaints Regarding the KMA-Wigdore Defendants’***  
11 ***Other Deceptive Marketing Practices***

12 145. EPS’s employees were aware of complaints regarding various other  
13 deceptive marketing practices, not related to the MNF scam, engaged in by the KMA-  
14 Wigdore Defendants and the sales agents working in Wigdore’s sales office. As early as  
15 December 19, 2011, one EPS employee emailed another EPS employee regarding a  
16 complaint received, stating: “New account we lost because Jay Wigdore lied.”  
17

18 146. In a February 22, 2012 email exchange between EPS employees regarding  
19 the “Wigdore accounts,” one EPS employee discussed two merchants: “Both of  
20 merchants have similar story, doing “lead generating” for Jay Wigdore . . . Dorothy  
21 Ventures isn’t a business. Both ladies are retired, damn near 90. I talked to Jordan in  
22 Q&A and Travis about these accounts . . . both agreed the accounts were are most likely  
23 opened fraudulently by the agent(s).”  
24

25  
26 147. In another email exchange between EPS employees, dated March 28, 2012,  
27 one employee described a consumer complaint received regarding false promises made  
28

1 by the Wigdore sales agent: “They are promising trips/cruises/getaways etc to merchants  
2 for signing up with EPS.” In reply, the other employee stated: “Yeah it’s well-known at  
3 this point.”

4  
5 148. In another email exchange between EPS employees regarding “Jay  
6 Wigdore Accounts,” dated September 11, 2012, one employee wrote: “We’ve seen an  
7 increase of non-installed merchants who are being signed up under false pretenses (agent  
8 2088).”

9  
10 ***EPS’s Principals, Defendants Thomas McCann and John Dorsey, and EPS’s Risk***  
11 ***Manager, Defendant Peterson, Personally Approved and Monitored the MNF***  
12 ***Merchant Accounts***

13 149. EPS Defendants Peterson, McCann and Dorsey directly participated in  
14 EPS’s central role in laundering transactions for the MNF scam.

15 150. EPS required Peterson, EPS’s Risk Manager, to closely track EPS’s client  
16 merchants’ sales and chargeback transaction activity on a regular basis. As noted above,  
17 various emails indicate that Peterson knew a great deal about the fraudulent nature of the  
18 businesses in which KMA and MNF were engaged, and their credit card laundering  
19 activities. Peterson received emails from Merrick in 2012, discussed above, in which  
20 Merrick expressed concern about KMA’s high chargeback rate “and the reason codes for  
21 them (services not provided)” and in which Merrick expressed the opinion that KMA was  
22 engaged in the unlawful practice of “load balancing.” In another email, Peterson  
23 expressed his conclusion that EPS should not fight a chargeback dispute involving a  
24 charge in the name of KMA Merchant Services for a “Rose Marketing” transaction,  
25 because “the argument against factoring is too great.” In another email, Peterson directly  
26  
27  
28

1 instructed Abdelmesseheh, acting in his capacity as EPS's sales agent, to "spread out"  
2 KMA's client merchant's transactions across multiple merchant accounts opened in the  
3 names of several MNF Fictitious Companies. Peterson also kept close track of the various  
4 EPS client merchants whose identities were concealed behind different company names,  
5 and was fully aware that many of the MNF Fictitious Companies were related to the same  
6 underlying merchant or individual.  
7

8  
9 151. Similarly, EPS's principals, Defendants McCann and Dorsey, approved and  
10 oversaw the MNF fraudulent merchant accounts, and personally met with the sales agents  
11 who referred the MNF Fictitious Companies to EPS.

12  
13 152. EPS did not have a separate department responsible for underwriting and  
14 approving merchant applications. Instead, EPS's principals, McCann and Dorsey,  
15 together with EPS's COO, were directly responsible for approving almost all merchant  
16 applications submitted to EPS for underwriting approval.  
17

18 153. Despite being EPS's Risk Manager, Defendant Peterson rarely had  
19 unilateral authority to approve any merchant applications. In fact, Peterson was generally  
20 required to obtain the approval of merchant applications from Defendants Dorsey or  
21 McCann, or EPS's COO.  
22

23 154. McCann and Dorsey personally met and communicated directly with the  
24 sales agents Wigdore and Abdelmesseheh. They each approved numerous merchant  
25 applications for the MNF Fictitious Companies referred by Wigdore—applications that  
26 contained glaring signs indicating the high probability that the fictitious companies were  
27 not legitimate businesses and were related to each other or to the same underlying  
28



1 merchant and, therefore, were likely being used to launder transactions for another  
2 merchant. As described above, in addition to numerous obvious signs that the purported  
3 merchants were not legitimate businesses, all the 2012 MNF Fictitious Company  
4 applications contained the facially suspect “Chase” checks—an obvious sign that the  
5 merchants likely were related to the same underlying merchant. Similarly, most of the  
6 2013 MNF Fictitious Company applications stated that each of the merchants banked at  
7 the same Wells Fargo Bank branch.  
8  
9

10 155. Dorsey personally approved numerous MNF Fictitious Company  
11 applications, including one merchant (Doc Assistant) whose application indicated that  
12 Wigdore was a co-owner or co-officer of the merchant, and that the merchant did not  
13 have a business website and owed a “past due amount” of \$20,225. Dorsey approved  
14 another merchant (Green Merchant Marketing), even though the merchant did not have a  
15 business website and owed a “past due amount” of \$139,463. Dorsey approved yet  
16 another merchant (V&R Marketing Solutions) who did not have a business website, owed  
17 a “past due amount” of \$10,914, and whose credit report indicated that the merchant’s  
18 address did not match the address listed on the application.  
19  
20

21 156. On July 24, 2012, Dorsey approved a merchant (Elite Marketing  
22 Strategies), despite the fact that the merchant’s incorporation papers indicated that the  
23 merchant had different owners and a different business address than those listed on the  
24 application. Moreover, an EPS employee had specifically noted that the merchant shared  
25 the same address as that of another EPS client merchant (JJB Marketing). EPS had  
26 previously processed for JJB Marketing just one month before, until it was instructed by  
27  
28

1 Merrick to terminate the merchant. Despite knowing that the new merchant was related to  
 2 the previous client merchant, Dorsey approved the application.

3 157. Similarly, McCann personally approved numerous MNF Fictitious  
 4 Company applications, including eight applications submitted by Wigdore within a span  
 5 of just two days (May 17, 2012 – May 18, 2012), two of which explicitly indicated that  
 6 Wigdore was a co-owner or co-officer of the merchant (A&D Marketing, Miller  
 7 Marketing Group), and five of which indicated that the merchant had the exact same  
 8 “KMA” email address (A&D Marketing, Global One Media, DePaola Marketing,  
 9 Wisdom Management Group, National Marketing Group). Two applications approved by  
 10 McCann indicated that the merchants shared the same business address, a fact highlighted  
 11 by the EPS employee who conducted the “initial risk evaluation” of the merchants.  
 12

13 158. McCann and Dorsey closely monitored the referral of new merchants to  
 14 EPS by EPS’s sales agents, as evidenced in daily emails (titled “Daily Hot Sheets”) sent  
 15 by EPS employees to McCann and Dorsey throughout 2013. These Daily Hot Sheets  
 16 provided McCann and Dorsey a daily log of all new merchants approved by EPS for  
 17 processing, and identified the ISO sales agent who referred the merchant to EPS. The  
 18 Daily Hot Sheets indicated that “Agent 2088” (KMA) was among EPS’s top sales agents  
 19 who were referring the highest number of merchant applications to EPS throughout 2013.  
 20

21 **EPS Transferred MNF Laundered Merchant Funds Into EPS Bank Accounts**  
 22 **Controlled By Dorsey and McCann**  
 23

24 159. In addition to receiving fees or commissions for opening the MNF  
 25 Fictitious Companies’ merchant accounts and processing transactions through them, EPS  
 26  
 27  
 28

1 transferred a substantial amount of MNF merchant funds (derived from MNF credit card  
2 sales generated by 16 of the fraudulent merchant accounts) into EPS's own bank  
3 accounts, which were jointly owned and controlled by Dorsey and McCann.  
4

5 **Defendants Are Jointly and Severally Liable For the MNF**  
6 **Transactions EPS Laundered Through Fraudulent Merchant Accounts**

7 160. Both the KMA-Wigdore Defendants and the EPS Defendants are jointly  
8 and severally liable for the harm caused to consumers when they laundered MNF  
9 transactions through the fictitious merchant accounts. Without the ISO and processing  
10 services provided by the Defendants, the MNF scam could not have obtained the  
11 fraudulent merchant accounts established at Merrick, which processed their credit card  
12 transactions.  
13

14 161. EPS processed a total of more than \$4,067,937 in sales transactions through  
15 the 2012 MNF Fictitious Company merchant accounts, the two KMA merchant accounts,  
16 and the Dynasty Marketing merchant account combined; and EPS processed more than  
17 \$1,827,098 for the 2013 MNF Fictitious Companies, for a combined total of more than  
18 \$5,895,035. These amounts do not include funds returned to consumers in the form of  
19 refunds or chargebacks.  
20

21 162. Many of the consumers whose credit cards were charged never obtained a  
22 refund or reversed charge for the unauthorized charges. Even those consumers who  
23 ultimately received a refund or reversed charge for the unauthorized charges were forced  
24 to expend valuable time and energy in requesting and seeking the refunds or chargebacks.  
25 In addition, these consumers' banks and the card networks also have incurred substantial  
26  
27  
28

1 economic harm as a result of expending time and energy processing requests for refunds  
2 or chargebacks.

3 163. Consumers who directly suffered economic harm as a result of the  
4 Defendants' actions could not reasonably have avoided such harm because (a) they were  
5 deceived by the deceptive telemarketing practices of the MNF scam, (b) they never  
6 authorized the MNF scam or the EPS Defendants to charge their credit card accounts in  
7 the names of the MNF Fictitious Companies, and (c) they had neither knowledge of nor  
8 control over the Defendants' actions in creating the MNF Fictitious Companies'  
9 merchant accounts through which Defendants processed MNF charges to the consumers'  
10 credit card accounts.

11 164. Credit card laundering is illegal and prohibited by the rules and policies of  
12 the credit card networks. No countervailing benefits flow to consumers or the credit card  
13 industry marketplace from the Defendants' conduct because no legitimate business  
14 purpose exists for credit card laundering.

### 15 VIOLATIONS OF THE FTC ACT

16 165. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or  
17 deceptive acts or practices in or affecting commerce." Acts or practices are unfair under  
18 Section 5 of the FTC Act if they cause or are likely to cause substantial injury to  
19 consumers that consumers cannot reasonably avoid themselves and that is not  
20 outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

### 21 COUNT I 22 (Against KMA-Wigdore Defendants)

- a) Falsely representing that the fictitious companies listed as the applicants on the merchant applications were the true merchants who were applying for merchant accounts; and/or
- b) Falsely representing that the fictitious companies listed as the account holders of the merchants' bank accounts on the merchant applications were the true account holders of the merchants' bank accounts.

168. Therefore, the Defendants' acts or practices, as described in Paragraphs 166 through 167 above, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and (n).

169. As described in Paragraphs 55 through 164 of this Complaint, in numerous instances, in connection with providing ISO or payment processing services to

merchants, Defendants Electronic Payment Systems, LLC; Electronic Payment Transfer, LLC; John Dorsey; Thomas McCann; and Michael Peterson have engaged in credit card laundering on behalf of the Money Now Funding scam by:

- a) Falsely representing that the fictitious companies listed as the applicants on the merchant applications were the true merchants who were applying for merchant accounts;
- b) Approving and opening multiple merchant accounts in the names of numerous fictitious companies for the same underlying merchant, thereby concealing the true identity of the underlying merchant; and/or
- c) Processing transactions for the same underlying merchant through multiple merchant accounts opened in the names of numerous fictitious companies, thereby concealing the true identity of the underlying merchant whose transactions were processed.

170. The Defendants' actions caused or were likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and that is not outweighed by countervailing benefits to consumers or competition.

171. Therefore, the Defendants' acts or practices, as described in Paragraphs 169 through 170 above, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and (n).

### VIOLATIONS OF THE TSR

172. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§

1 6101-6108. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively  
2 amended it in 2003, and amended certain provisions thereafter. 16 C.F.R. Part 310.

3 173. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and  
4 Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR  
5 constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of  
6 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).  
7

8 174. Under the TSR, a “merchant” means a person who is authorized under a  
9 written contract with an acquirer to honor or accept credit cards, or to transmit or process  
10 for payment credit card payments, for the purchase of goods or services or a charitable  
11 contribution. 16 C.F.R. § 310.2(u).  
12

13 175. The MNF Fictitious Companies and Defendants KMA Merchant Services,  
14 LLC, Michael Abdelmessehe, Dynasty Merchants, LLC, and Nikolas Mihilli were  
15 “merchants” who entered into “merchant agreements,” as those terms are defined by the  
16 TSR, 16 C.F.R. § 310.2(u)–(v).  
17

18 176. The MNF Fictitious Companies were “seller[s]” or “telemarketer[s]”  
19 engaged in “telemarketing,” as those terms are defined in the TSR, 16 C.F.R. §§  
20 310.2(dd), (ff), and (gg).  
21

22 177. Except as expressly permitted by the applicable credit card system, it is a  
23 deceptive telemarketing act or practice for:  
24

- 25 a) a merchant to present to or deposit into, or cause another to present to or  
26 deposit into the credit card system for payment, a credit card sales draft  
27 generated by a telemarketing transaction that is not the result of a  
28

1 telemarketing credit card transaction between the cardholder and the  
 2 merchant; or

3 b) any person to employ, solicit, or otherwise cause a merchant, or an  
 4 employee, representative or agent of the merchant, to present to or deposit  
 5 into the credit card system for payment, a credit card sales draft generated  
 6 by a telemarketing transaction that is not the result of a telemarketing credit  
 7 card transaction between the cardholder and the merchant. 16 C.F.R. §§  
 8 310.3(c)(1)–(2).  
 9  
 10

11 178. The TSR prohibits any person from providing substantial assistance or  
 12 support to any seller or telemarketer when that person knows or consciously avoids  
 13 knowing that the seller or telemarketer is engaged in acts or practices that violate  
 14 Sections 310.3(a), (c) or (d), or Section 310.4 of the TSR. 16 C.F.R. § 310.3(b).  
 15

16 **COUNT III**  
 17 **(Against All Defendants)**

18 179. In numerous instances, and without the express permission of the  
 19 applicable credit card system, the Defendants have employed, solicited or otherwise  
 20 caused the MNF Fictitious Companies, or representatives or agents of the MNF Fictitious  
 21 Companies, to present to or deposit into, the credit card payment system for payment, a  
 22 credit card sales draft generated by a telemarketing transaction that is not the result of a  
 23 telemarketing credit card transaction between the cardholder and the MNF Fictitious  
 24 Companies, as described in Paragraphs 55 through 164 above.  
 25  
 26  
 27  
 28



**COUNT IV**  
**(Against KMA Merchant Services and Michael Abdelmesseh)**

182. KMA Merchant Services, LLC's and Michael Abdelmesseh's acts or practices, as described in Paragraph 181 above, are deceptive telemarketing acts or practices, that violate the TSR, 16 C.F.R. § 310.3(c)(1).

**COUNT V**  
**(Against Dynasty Merchants, LLC and Nikolas Mihilli)**

54

1           184. Dynasty Merchants, LLC's and Mihilli's acts or practices, as described in  
2 Paragraph 183 above, are deceptive telemarketing acts or practices, that violate the TSR,  
3 16 C.F.R. § 310.3(c)(1).  
4

5                                   **COUNT VI**  
6                                   **(Against All Defendants)**

7           185. In numerous instances, Defendants provided substantial assistance or  
8 support to sellers and telemarketers (the MNF Fictitious Companies, or representatives or  
9 agents of the MNF Fictitious Companies) that the Defendants knew, or consciously  
10 avoided knowing, were engaged in credit card laundering acts or practices that violate  
11 Sections 310.3(c)(1) and (2) of the TSR, as described in Paragraphs 55 through 164  
12 above.  
13

14           186. Defendants' acts or practices alleged in Paragraph 185 above constitute  
15 deceptive telemarketing acts or practices, in violation of the TSR, 16 C.F.R. § 310.3(b).  
16

17                                   **CONSUMER INJURY**

18           187. As described in Paragraphs 55 through 164 above, consumers throughout  
19 the United States have suffered and will continue to suffer substantial injury as a result of  
20 the Defendants' violations of the FTC Act and the TSR. In addition, Defendants have  
21 been unjustly enriched as a result of their unlawful acts and practices. Absent injunctive  
22 relief by this Court, Defendants are likely to continue to injure consumers, reap unjust  
23 enrichment, and harm the public interest.  
24  
25  
26  
27  
28

## THE COURT'S POWER TO GRANT RELIEF

188. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

189. Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the TSR, including the rescission or reformation of contracts, and the refund of money.

## PRAYER FOR RELIEF

190. Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), and the Court's own equitable powers, requests that the Court:

- a) Award Plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief;
- b) Enter a permanent injunction to prevent future violations of the FTC Act and the TSR by Defendants;

- 1 c) Award such relief as the Court finds necessary to redress injury to  
2 consumers resulting from Defendants' violations of the FTC Act and the  
3 TSR, including, but not limited to, rescission or reformation of contracts,  
4 restitution, the refund of monies paid, and the disgorgement of ill-gotten  
5 monies; and  
6  
7 d) Award Plaintiff the costs of bringing this action, as well as such other and  
8 additional relief as the Court may determine to be just and proper.  
9

10 DATED this 9th day of March, 2018.

11  
12  
13 /s/ Michelle Chua  
14 Michelle Chua  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28